



EnCoRe Publication

Title: Privacy and informed consent in online interactions: Evidence from expert focus groups

Authors: Edgar A. Whitley and Nadja Kanellopoulou

Date: September 2010

Publication Details: To appear in the International Conference on Information Systems, 2010, St Louis, Missouri.

Summary: This paper draws on evidence from a series of expert focus groups to question the function of “informed consent” in online transactions. Informed consent and related concepts have a key role in much privacy research and are an integral part of much data protection legislation. The research methodology used in this paper was focus groups with expert participants and the paper describes this approach in detail. Four expert groups, with participants from civil society organizations, data protection professionals, public sector organizations and small and medium sized enterprises (SMEs) took part in the focus groups which ran for a total of 10 hours. This paper reports on the results from the focus groups in terms of a) privacy policies, b) control over the use of personal data, c) consent as a response to regulatory requirements and d) the nature of informed consent. The evidence from the focus groups questions the extent to which informed consent operates in online interactions. This suggests a number of novel research directions that arise from the analysis. The paper ends by suggesting alternative ways of addressing “informed consent” in online interactions.

PRIVACY AND INFORMED CONSENT IN ONLINE INTERACTIONS: EVIDENCE FROM EXPERT FOCUS GROUPS

Completed Research Paper

Edgar A. Whitley

Information Systems and Innovation
Group,
Department of Management,
London School of Economics and Political
Science,
Houghton Street, London WC2A 2AE,
United Kingdom
e.a.whitley@lse.ac.uk

Nadja Kanellopoulou

Centre for Health, Law and Emerging
Technologies at Oxford (HeLEX),
Department of Public Health,
University of Oxford,
Old Road Campus,
Oxford OX3 7LF,
United Kingdom
Nadja.Kanellopoulou@dphpc.ox.ac.uk

Abstract

This paper draws on evidence from a series of expert focus groups to question the function of “informed consent” in online transactions. Informed consent and related concepts have a key role in much privacy research and are an integral part of much data protection legislation. The research methodology used in this paper was focus groups with expert participants and the paper describes this approach in detail. Four expert groups, with participants from civil society organizations, data protection professionals, public sector organizations and small and medium sized enterprises (SMEs) took part in the focus groups which ran for a total of 10 hours. This paper reports on the results from the focus groups in terms of a) privacy policies, b) control over the use of personal data, c) consent as a response to regulatory requirements and d) the nature of informed consent. The evidence from the focus groups questions the extent to which informed consent operates in online interactions. This suggests a number of novel research directions that arise from the analysis. The paper ends by suggesting alternative ways of addressing “informed consent” in online interactions.

Keywords: Privacy, Informed Consent, Focus Groups, Organizational Practices

This work was supported by the Technology Strategy Board; the Engineering and Physical Sciences Research Council and the Economic and Social Research Council [grant number EP/G002541/1]. We would like to thank our colleagues on the EnCoRe project for the many insightful comments they have contributed. Particular thanks are due to Patrizia Bertini, Liam Curren, Jane Kaye and Prodromos Tsiavos for their inputs into this paper. Additional feedback was received following a presentation of this work at PUMP 2010.

Introduction

On 9 February 2010, the advertising and search company Google launched its Buzz service as part of its web-based mail service. Buzz was intended to be a “social networking” add-on, allowing mail users to share personal information in a similar manner to Facebook and Twitter. Within days, however, data subjectsⁱ were expressing concerns about the service, claiming that it invaded their privacy (Fiveash, 2010). In April 2010, privacy and data protection regulators from Canada, France, Germany, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain and the United Kingdom wrote an open letter to Google expressing their concern at the way “the privacy rights of the world’s citizens are being forgotten as Google rolls out new technological applications” as these represent a “disregard for fundamental privacy norms and laws” (Open letter, 2010). This unprecedented, collaborative response from these various regulators was in part a recognition of the severity of the fact that users were not given a choice about opting-in to the service, instead, Buzz was automatically “added” as part of their mail service.

Although Google has since claimed that the problems with Buzz were simply a result of testing flaws (BBC News, 2010a), the case illustrates the increasingly important issue of how organizations collect and use personal data about their customers. In particular it calls into question the extent to which Google’s actions meant that their customers were giving their informed consent when Buzz was added to the online services they were using.

The concept of consent as informed consent has been widely studied in medicine and bioethics more generally, and is frequently implicit in discussions of privacy and data protection in the context of personal data and online interactions. In medical treatment and research, consent is to be secured as the individual’s free and informed choice, through communication and apprehension of the risks and benefits of a particular medical intervention. Extensive debate exists about the nature, scope and usefulness of consent in medicine (Jackson, 2009; Mason & Laurie, 2006). What is less well understood, however, is how informed consent can function in the context of online services more widely and, particularly, how commercial organizations and public sector bodies implement the gathering and management of consent from their customers and citizens.

This paper reports on an exploratory, qualitative study undertaken in the UK as part of a larger research project. The study took the form of a series of focus groups that sought to elicit the opinions of various expert groups with regard to the operation and applicability of informed consent in online interactions. The focus groups were designed to draw out perspectives from civil society organizations, data protection professionals, commercial organizations and the public sector in the UK. The paper contributes to our understanding of consent, privacy and data protection in the context of online interactions including registration with online services, targeted advertising and other third party uses of personal data. It calls into question the current thinking of informed consent for online interactions and suggests that new ways of thinking about mechanisms through which data subjects might control how their data is used by organizations are needed.

The structure of the paper is as follows: after introducing the concept of informed consent, the paper reviews the literature and related empirical studies about privacy and data protection as they relate to consent. This review gives rise to a series of research questions. After presenting details of the research project, the paper describes the data collection and analysis methods associated with the focus groups. A discussion of the results of the focus groups, as they relate to the research questions follows. The paper concludes with a discussion of the implications of this analysis for current theory and practice.

Understanding informed consent

In seeking to understand how consent functions in the management of online interactions, it is useful to refer briefly to its origins and rationale in medical research since historically the term obtained its first use within that tradition. In 1964, the World Medical Association developed an authoritative definition of informed consent in the context of medical research:

In medical research involving competent human subjects, each potential subject must be adequately informed of the aims, methods, sources of funding, any possible conflicts of interest, institutional affiliations of the researcher, the anticipated benefits and potential risks of the study and the discomfort it may entail, and any other relevant aspects of the study. The potential subject must be informed of the right to refuse to participate in the study or to withdraw consent to participate at any time without reprisal. Special attention should be given to the specific information needs of individual potential subjects as well as to the methods used to deliver the information. After ensuring that the potential subject has understood the information, the physician or another appropriately qualified individual must then seek the potential subject's freely-given informed consent, preferably in writing. If the consent cannot be expressed in writing, the non-written consent must be formally documented and witnessed (World Medical Association, 1964).

According to Hoeyer (2009), the institutional "myth" behind informed consent in the context of medicine is that it arose in response to the dreadful experiments undertaken by Nazi doctors in German concentration camps during World War Two. Following an International Military Tribunal, the Nuremberg Code was developed in which the right of a research subject to give a voluntary consent (§1) and the right to withdraw from research (§9) were clearly established. These requirements were intended to respect the autonomy of the individual and provide a safeguard against the kinds of experiments that had been undertaken in the concentration camps.

Despite informed consent having been articulated some forty years earlier, and the fact that the Allied Forces had conducted its own dangerous experiments on prisoners (presumably without their informed consent), the Nuremberg code had little impact on the medical profession chiefly because it was perceived as a response to Nazi excesses ("a good code for barbarians but an unnecessary code for ordinary physician-scientists" (Katz, 1992 p. 228)). By the 1960s, however, developments in medical research and concern about regulative interference led to the Helsinki Declaration in 1964 by the World Medical Association (World Medical Association, 1964) and, as Hoeyer notes, this has become the norm for medical research.

Comparatively, while investigating the concept of consent in the context of online interactions, a similar ideal can be articulated at first instance:

In online interactions, each potential data subject must be adequately informed of the aims and methods of the service provider, the anticipated benefits and potential risks of the interaction and any other relevant aspects of the interaction. The potential data subject must be informed of the right to refuse to participate in the interaction or to withdraw consent to participate at any time without reprisal. Special attention should be given to the specific information needs of individual potential data subject as well as to the methods used to deliver the information. After ensuring that the potential data subject has understood the information, the organization must then seek the potential subject's freely-given informed consent.

A core element of such a definition of online informed consent would be the need for the data subjects to be adequately informed about what they are signing up for, including benefits and risks. The means by which this informing process is undertaken need to be clear and appropriate. Data subjects must be aware of the consequences of not giving consent and the data subject must actively provide

their freely-given consent. Bearing these considerations in mind about informed consent in online interactions the aim of our focus group research was to explore the views of expert participants by drawing on the perspectives of data subjects and data controllers.

Privacy and data protection

Although the terms data protection and privacy are often used interchangeably, especially in the management literature (see, for example, Kuner, 2003) they are not identical, particularly in the European context. Privacy can be described as “a condition or state in which a person (or collective entity) is more or less inaccessible to others, either on the spatial, psychological or informational plane” (Bygrave, 2002 p. 23), data protection is defined as “a set of measures (legal or non-legal) aimed at safeguarding persons from detriment resulting from the processing (computerized or manual) of information on them” (Bygrave, 2002 p. 22).

Privacy

Introna’s (1997) review of the literature on privacy suggests that there are three broad categories of privacy definitions: privacy as no access to the person or the personal realm; privacy as control over personal information and privacy as freedom from judgment or scrutiny by others.

Legal theorists have drawn on earlier discussions of the distinction between public and private realms to highlight some of the implications of this distinction in terms of legal rights. One of the earliest and most significant was the argument by Samuel Warren and Louis Brandeis (1890) who developed a right of privacy, namely “the right to let alone”. This was based on an earlier judgment by Thomas Cooley who proposed “the right to one’s person and a right of personal immunity” (see DeCew, 1997 p. 14). That is, they saw privacy as closely related to being able to control actions and information about oneself. Privacy is thus associated with notions of personhood and self-identity (Kanellopoulou, 2009 p.2).

Introna’s second definition highlights what is often described as informational self-determination (De Hert, 2008), based on a 1983 ruling by the German Federal Constitutional Court. The argument here is that if an individual cannot reasonably control how their information is used (for example, if it is subject to searches by the authorities) then they may refrain from undertaking socially useful information-based activities such as blogging on particular topics.

The third category, freedom from judgment by others, again relates to the disclosure and use of personal data by others. For example, in this category personal health data might reasonably be considered private because its involuntary disclosure may cause others to judge an individual’s lifestyle choices.

Whilst many scholars see privacy as having intrinsic value as a human right, something that is inextricably linked to one’s essence as an (autonomous) human being, others highlight a more instrumental role for privacy such as protection of one’s independence in making important personal decisions, for example when undertaking commercial activities. This claim is not always just instrumental (Allen, 1999) and it is considered as intrinsic for the protection of the development of one’s personality (Kanellopoulou, 2009 p. 4).

More generally, privacy concerns have frequently been linked to questions of trust in online interactions. For example, it is widely recognized that online interactions are more likely to succeed if the parties to the interaction trust one another (Pavlou, 2003) because the principal-agent dilemma of information asymmetry applies. In business-to-consumer (b2c) electronic commerce transactions

information privacy concerns can help explain a substantial degree of perceived uncertainty in transactions (Pavlou et al., 2007). An example of an informational privacy concern in a b2c relationship is worry about how the bank account data provided by the data subject are going to be stored and used by the business. Concerns about informational privacy are not limited to financial details and can include health records (Angst & Agarwal, 2009), business transactions (Hoffman et al., 1999), social networking practices (Light et al., 2008) and government databases (FIPR, 2009).

Empirical studies about privacy and consent

Empirical research that studies how consent affects behavior are widespread in the medical and bioethics literature (e.g. Veatch, 2007; Moskop, 2007; Wilkinson, 2001; Zeps et al., 2007) as well as the marketing literature (e.g. Petty, 2000; Pollach, 2005). With technological changes, including the internet and social networking sites, there has also been a resurgence in empirical studies of informational privacy and related issues (e.g. Hoofnagle et al., 2010; Tsai et al., 2010). Many of these studies focus on individual perceptions of privacy and may not explicitly address issues of consent. Others do explicitly seek to study consent, for example by focusing on procedural fairness (e.g. Culnan & Armstrong, 1999) or innovative empirical settings such as location-based services (Junglas et al., 2008).

A dominant theme in the information systems literature is the development of a model of privacy concerns. For example, Smith et al. (1996) present the development and validation of a research instrument that identifies and measures the primary dimensions of concern with organizational practices regarding informational privacy, drawing on, amongst other things, Fair Information Practices. Whilst some of the items on their instrument relate to general data concerns (data accuracy, excessive data collection etc.) they also have specific items that can be recast in terms of consent. For example, item C states “Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information”; item G states “When people give personal information to a company for some reason, the company should never use the information for any other reason” and item M says “Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information”.

Malhotra et al. (2004) develop the existing marketing literature about privacy concerns (e.g. Petty, 2000) and apply them to the internet age to examine “internet users’ information privacy concerns (IUIPC)”. This extends the four dimensions (collection, errors, unauthorized secondary use, improper access) of the concerns for information privacy identified by Smith et al. (1996). Malhotra et al. propose that an individual’s concerns for information privacy include consideration of whether the individual has “control” over personal information. This control, they suggest, can be seen by the existence of voice (i.e., approval, modification) or exit (i.e., opt-out) (cf Whitley, 2009). They also use social contract theory to highlight the importance of data subjects being informed about the organization’s intended use of the data which they label as “awareness”.

Culnan and Armstrong (1999) examine the tensions in the collection and use of personal data by organizations. They suggest that organizations that offer perceived “procedural fairness”—which acts as an intermediary between the customer and the organization—mitigate the trust concerns about the use of personal data that can arise in such situations (see also Culnan, 1993). They suggest that procedural fairness might take the form of the organization adopting the Fair Information Practices outlined below. In their empirical study of the perceptions of 1000 U.S. adults, when organizations implement the principles of notice and consent from the Fair Information Practices “only prior experience distinguished individuals who were willing to be profiled from those who were not willing” (Culnan & Armstrong, 1999 p. 112). In a similar manner, Hui et al. (2007) explore the extent

to which privacy statements and privacy seals, that act as a proxy for procedural fairness, affect the disclosure of personal data. Their study suggests that the existence of a privacy statement is more likely to induce the disclosure of personal data, whilst the existence of privacy seals has no effect.

Son and Kim (2008) present a series of information privacy–protective responses to the perception of information privacy threats that can arise from an organization’s information practices. In the context of consent and privacy, their discussion of private actions that individuals can take includes discussion of using opting–out procedures. In response to these kinds of actions, the authors recommend that organizations “implement fair procedures to protect the information privacy of customers” and be “trustworthy and honest in dealing with the information privacy of customers” (Son & Kim, 2008 p. 520).

An alternative research approach to quantitative surveys is deliberative research. For example, Bradwell (2010) reports on a deliberative “people’s inquiry” that involved 40 people in a month–long process that ran for 13 hours of expert presentations, discussions and reflection. This study found that the participants had “conditional faith” in the use of personal data by the public sector and “wary skepticism” in their relationship with the private sector. That is, their skepticism about how the private sector would use their data meant that they felt there was a greater need for informed and explicit consent to be obtained when interacting with private sector organizations.

Data protection

The processing of personal data is heavily influenced by changes in information and communications technologies. Different stages in the evolution of ICTs have provoked different modes of processing and communication of personal data and different institutional response to the perceived threats to personal data. From the mainframes of the 1970s that gave rise to the first data protection regulations, to personal computing, the internet and then web 2.0 technologies, data protection regulation has known consecutive related changes in the direction of greater decentralization of processing, storage and communication of information.

The German federal state of Hessen enacted one of the first data protection laws in 1970 (Kuner, 2003 p. 13). In the UK, the Younger Committee on Privacy (Younger Committee, 1972) also considered the threat of computers on personal privacy (Collins, 1993). Another early response was the development of “Fair Information Practices” which emerged from a 1973 report published by the U.S. Department of Health, Education and Welfare (U.S. Department of Health Education and Welfare (HEW), 1973). These principles are technology–independent procedural guarantees which attempt to balance the rights of individuals with those of organizations (Culnan, 1993).

The HEW principles state that: individuals should have the right to know how organizations use personal information and to inspect their records and correct any errors; individuals should have the right to prevent secondary use of personal information if they object to such use; and organizations that collect or use personal information must take reasonable precautions to prevent misuse of the information (Culnan, 1993).

The HEW Fair Information Practices were developed further in a document produced by the OECD in 1980 (OECD, 1980; Bonner & Chiasson, 2005). The document was explicitly designed as a response to “development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents”. It noted that whilst privacy protection laws were being introduced by one half of OECD Member countries there was a danger that disparities in national legislations could hamper the free flow of personal data across frontiers.

Such restrictions on data flows “could cause serious disruption in important sectors of the economy, such as banking and insurance”. The Guidelines were therefore intended to “help to harmonize national privacy legislation” and would do this whilst both upholding human rights and preventing interruptions in international flows of data. The Guidelines were intended to represent a consensus on basic principles which can be built into existing national legislation (Curren, 2009).

Within Europe similar considerations gave rise to the introduction of the Council of Europe Convention of 1981 that provided, in turn, the impetus for the first UK Data Protection Act in 1984. A decade later, the EU revised its stance on data protection with a new directive. The principal aim of national data protection laws, according to the Data Protection Directive (95/46/EC) should be to ensure the protection of individuals’ privacy when their personal data are handled by third parties. The reference to privacy is present in the Directive because the Directive is intended to link with Article 8 of the European Convention of Human Rights (ECHR): “the right to respect for private and family life”.

The Data Protection Act 1998 is the primary piece of legislation to implement the Directive in the UK but it fails to mention the word privacy even if it must be assumed to fulfill the aim of the Directive through its use of a series of “privacy–friendly” data processing principles (Curren & Kaye, 2010).

Common to each of these approaches is the consideration of the individual’s right to prevent secondary uses of personal information (HEW) or, as the OECD guidelines state: collection and use of personal data is limited by a requirement to obtain the explicit prior consent of the individual. In the context of organisational practices, it has been shown that providing enhanced consumer control over the uses of their personal data, through a combination of opt–in policies and “informed consent” is likely to provide the largest financial benefits for organisations (Hoffman et al., 1999; Awad & Krishnan, 2006).

There is, however, a tension behind the use of informed consent and opt–in approaches to address the human rights angle of individual autonomy and the commercial / compliance / audit angle where obtaining consent helps demonstrate compliance with, in this case, Fair Information Practices and relevant data protection regulations (Culnan & Armstrong, 1999).

Organizational perspectives on data protection

Complementing the studies of individual privacy behaviors, there is also a growing literature of organizational perspectives and practices on informed consent for online interactions. For example, in North America the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants recently released the Generally Accepted Privacy Principles (GAPP) (Culnan & Williams, 2009). Principle 2 “notice” states that “the organization [has] to provide notice about its privacy policies and procedures. This includes the purpose(s) for which personal information is collected, used, retained, and disclosed” whilst Principle 3 “Choice and consent” requires the organization to describe “the choices available to the individual related to the use and disclosure of their information, and to obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information”.

Given the nature of Data Protection / Privacy regulation in North America, the adoption of these principles is voluntary (AICPA, 2010). In contrast, within Europe the OECD guidelines and Fair Information Practices have been realized as Data Protection Directives and then implemented as national Data Protection Laws. For example, the UK Data Protection Act states that “Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further

processed in any manner incompatible with that purpose or those purposes” (OPSI, 1998 Principle 2 in Schedule 1 of the Act). Whilst the GAPP is entirely voluntary, compliance with the Data Protection Act is compulsory with an independent regulator, the Information Commissioner’s Office, which reports directly to the UK Parliament (Information Commissioner's Office, 2010). Failure to comply with the Act can result in financial penalties and reckless misuse of personal data is due to lead to custodial sentences.

Like other European data protection regulators, the ICO does not see its goal as primarily one of penalizing miscreants; rather a key role in its strategy is providing guidance and support for organizations about how to organize their practices so that they comply with the Act. (Naturally, the ICO also provides support and guidance for individuals about their rights under the Act). For example, the ICO recently issued a Privacy Notices Code of Practice (Information Commissioner's Office, 2009) that gave detailed advice on good and bad practice on privacy notices. For example, they advise that “You should always be straight with the public” but also note that there is a fundamental difference “between telling a person how you’re going to use their personal information and getting their consent for this. In many cases it is enough to be transparent. In other cases a person’s positive agreement will be needed”. Consent, they suggest is likely to be required in situations where “sensitive information is being collected, or where previously collected information is to be used in a significantly different way” (Information Commissioner's Office, 2009 p. 8). A recent example of this is the case of the gay teenager magazine XY, whose database of registered site users was deemed one of the firm’s remaining valuable assets by creditors (BBC News, 2010b).

The British Computer Society has also issued a personal data guardianship code (BCS, 2009) which again provides support to organizations wishing to comply with the Data Protection Act. Thus, they advise that the person responsible for data in an organization (the “Data Controller” in the terms of the Act) “should ensure that their organization explicitly secures the consent of personal data subjects before storing and / or accessing personal data. They should also ensure that they have consent to share with third parties, if they intend to do so (other than where they are legally obliged to pass personal data on to government bodies)”.

Implementing effective mechanisms for obtaining an individual’s consent can be problematic. For example, the EU Article 29 Working Party recommended that search engine providers must obtain consent from their users before engaging in any data collection or profiling (EU, 2008). This recommendation raised particular technological challenges because it was intended to apply to both authenticated and non-authenticated users.

Another technological concern is the extent to which consent can, or should be, engineered (Kerr et al., 2009). That is, are there contextual factors that nudge the behavior of normal individuals towards particular kinds of options (cf Thaler & Sunstein, 2008), for example, preferring instant gratification over future threats? More generally this raises questions about whether the default position should be to require opt-in or opt-out consent, i.e. whether consent can be presumed (Veatch, 2007).

Lundblad and Masiello (2010) highlight how a simple requirement in favour of opt-in can lead to social welfare problems. Whilst opt-in consent can be easily sought when, for example, registering for an online service (as part of the terms and conditions or explicitly), there is a risk that a) the consent given will, by necessity, be unduly broad to cover all potential future uses; b) once consent is obtained there is no incentive for the service provider to seek confirmation that the consent still holds; and c) consent must be provided before the data subject can “try out” the service. In non-authenticated situations, requiring opt-in can be unsatisfactory from a usability perspective (try

setting your browser's privacy level to "ask me before accepting cookies" and then visit any commercial website that hosts adverts).

Research questions

The focus groups generated a significant amount of research data. For the purposes of this paper, a subset of this data is presented so as to maintain narrative coherence (cf Law & Mol, 2002). Thus, this section presents a reconstructed subset of the research questions / themes that were explored in the focus groups. Themes from the focus groups that are not covered in this paper—but which fed into other parts of the project—include the role of meta-data, different forms of contractual / licensing arrangements for the use of personal data and user interface considerations. Our review of the literature on privacy and data protection provides concrete insights into the ways in which informed consent can or cannot be found in current online interactions. This research gives rise to a series of further specific issues that our expert focus group participants sought to address:

Theme 1: *Privacy policies, terms and conditions*

- To what extent do privacy statements provide an adequate way to inform all potential data subjects about the decision they are about to make?
- To what extent do privacy statements provide details of the aims and methods of the service provider and the benefits and risks of the interaction?

Theme 2: *Effective control over use of personal data*

- How much control do data subjects have over the use of their personal data?
- To what extent are data subjects informed of the consequences of refusing to provide their consent?

Theme 3: *Consent as a response to regulatory requirements*

- If consent is obtained, what purpose does the collection of consent address?
- How effective are the specific regulatory interventions found in the UK for ensuring informed consent?

About the project: EnCoRe: Ensuring Consent and Revocation

The research presented in this paper is part of a 45 month research project. EnCoRe (<http://www.encore-project.info>) is a multi-disciplinary research project, spanning across a number of IT and social science specialisms, and researching how to improve the rigor and ease with which individuals can grant and, more importantly, revoke their consent to the use, storage and sharing of their personal data by others.

As more and more personal information flows from individuals to organizations when they interact online, people become increasingly concerned that they cannot effectively control what this information is used for, with which other organizations it is shared and where it is stored. They may have given their consent, often in vague terms and implicitly, for its use, sharing and storage, but they have no real control over the specifics of these, nor the ability to revoke their consent and be sure that their wishes are respected. In summary, individuals are not able to control where their personal information flows to, an issue which can cause unease about interacting online.

The overall vision of the EnCoRe project is to make giving consent as reliable and easy as turning on a tap, and revoking that consent as reliable and easy as turning it off again. The research in this project is conducted through three scenarios as applied case studies. Each case study investigates

differing factors and requirements for reliable consent and revocation mechanisms and running prototype solution design / build / verify cycles on them.

EnCoRe emerged from a specially facilitated week long “sandpit” that brought together researchers from various disciplines as well as industry representatives. The sandpit was run by specialist facilitators and employed a series of innovative practices to develop and to peer-review research ideas in an intensive and interactive format. The project partners are Hewlett-Packard Laboratories, HW Communications, QinetiQ, the London School of Economics, the HeLEX Centre at the University of Oxford and the University of Warwick e-security group. The project runs from June 2008 to February 2012. It receives funding from the UK Government’s Technology Strategy Board, Economic & Social Research Council and Engineering & Physical Sciences Research Council.

Empirical data collection

This study draws on empirical data from four selected focus groups with expert rather than lay participants. Although widely practiced in marketing research, the application of focus groups methodologies to information systems research in general, and privacy research in particular, has been surprisingly limited. Indeed, in this mainstream literature, if used at all, focus groups are frequently applied in an informal, ad hoc way that fails to take full advantage of the opportunities that this method affords. In addition, in information systems research focus groups are normally applied in conjunction with other data collection techniques. This section therefore introduces the focus group approach to data collection as a relatively novel research approach (Tams & Grover, 2010), before describing the characteristics of the four expert groups and how they were run, as well as the methods that were used to analyze the data generated.

Focus groups as a methodological approach to data gathering

As a research method, focus groups provide the opportunity for the collection of detailed, qualitative data about a particular product, concept or innovation and offer distinct advantages over individual interviews (Williams, 2003). They are intended to be interactive activities whereby differing viewpoints and perspectives emerge from the interaction between focus group participants. As such focus groups are a powerful and flexible means to generate hypothesis, explore opinions, ideas or attitudes, test new products or concepts (Fern, 1982 p. 1).

Focus groups are an organized discussion (Gibbs, 1997) which capitalizes on communication between research participants in order to generate data based on group interaction (Kitzinger, 1995 p. 311). As a consequence they are particularly useful for revealing different perspectives, beliefs and attitudes, for example when one person’s contribution triggers responses from other participants (Gibbs, 1997; Fern, 1982).

These attitudes and perceptions are developed, in part, by a structured process of interaction with others in the group that would not be expected to emerge in a sequential series of one-on-one interviews with the same individuals (Krueger, 1988). This means that the unit of analysis is the group rather than the individual (Perecman & Curran, 2006 p. 107). In some cases group interaction might cause individual perceptions and opinions held by focus group members to shift over time, changes which the focus group process can help document quite effectively. In contrast to other group-based participatory methods (such as the Delphi method or brainstorming) the purpose of a focus group is *not* to arrive at a decision in a group consensus or to provide recommendations (cf Tremblay et al., 2010).

The groups are termed to be focused because the data that are collected depend on group interaction as a central part of the method itself (Kitzinger, 1994; Kitzinger, 1995).

The extensive literature on focus groups recommends that groups should be composed of at least six participants, with most authors proposing between five and twelve participants as the ideal number (Morgan, 1993). Very large focus groups can be unproductive as it may be difficult to include contributions from all participants and there may be a tendency for the discussion to fragment and a series of mini-conversations to emerge (Krueger, 1988). Very small focus groups are unlikely to reveal significant insights from the group process as they can effectively become a series of individual interviews.

Selection of focus group participants is important. Traditionally, the rationale for developing focus groups methods was that the participants should not know each other beforehand because communication issues—such as organizational power-dynamics—might affect what is disclosed and discussed in the group (Albrecht et al., 1993). Beyond this constraint, existing advice recommends forms of sampling for lay groups (e.g. a mix of genders, ages or roles) as appropriate for encouraging diversity of opinions during the focus group session and consequently, an emergent, evolving discussion (Krueger, 1993). More recently, and in particular for cases of organizationally-based focus groups, it has been recognized that it might not be practical to create groups of individuals who do not know each other and that, in such cases, particular care must be taken with group facilitation so as to ensure that such pre-existing relationships do not affect the discussion.

Managing the dynamics of focus groups requires specialist skills that are not necessarily well developed by generalist researchers. Since there is no intention in focus groups research to arrive at a decision or series of recommendations, it is important that the facilitator of the focus group creates a permissive environment that nurtures different perceptions and points of view without needing to reach consensus. The facilitator needs to ensure that they do not give any implicit support or recognition of particular viewpoints or speakers as this might limit the contributions, in the discussion, of other participants, and other perspectives (Krueger, 1988). This care can involve subtle body language or even using phrases like “uh huh” rather than “yes” or “thank you” when responding to particular individuals. The facilitator may also address group dynamics by sitting next to particular participants or deliberately paying less attention to individuals who have been identified as likely “conversation hogs”. Furthermore, a good facilitator is expected to be able to elicit insights and comments from apparently quieter members of the focus group.

In structuring the focus group discussion, it is common to develop an interview agenda that would be “deceptively simple” but actually is carefully designed to help structure and control the discussion over time. As with all such instruments, pre-testing for comprehension ability and timing is beneficial. A typical focus group preparation might involve a dozen structured questions—although fewer may be required if responses on specific issues are sought for or if the participants are particularly knowledgeable or experienced in the targeted area of research (Krueger, 1993). Including a break for refreshments also allows time for reflection on whether the discussion is keeping to the agreed agenda or if remedial action is required to bring the conversation back to the topic of concern (Krueger, 1993). Presenting a summary of the discussion before closing and allowing all participants to add anything that “might have been missed” helps both to provide a quick quality check that the main thrusts of the discussion have been understood correctly as well as flagging up other issues that did not emerge in the course of group discussion (Krueger, 1993).

To support the facilitator, it is common to have a second person involved as a “note-taker”. This individual can focus on the content of the discussion rather than how it is being run and is a useful back up in case the recording devices fail. Depending on the requirements of the focus group, it is common for the focus group discussion to be recorded (audio and / or video) and for it to be transcribed. As with all such recordings, the informed consent of participants is required. They need to be told about how the recording will be used and whether comments made by them will be attributed or not. In addition, problems of failing recorders, poorly placed microphones, conversations taking place out of microphone range or being overwhelmed by situational noise (traffic, air conditioning etc.) might affect the quality of the recording and hence of any transcription.

The EnCoRe expert focus groups: Selecting participants

Although non-expert focus groups are generally the norm, given the particular emphasis of the EnCoRe project on the issue of consent, it was felt that it would be more appropriate to host a series of focus groups with experts. That is, the participants would be chosen as individuals who have already developed a detailed awareness of some of the complexities associated with privacy and consent. Thus the focus group process sought to gather informed opinions rather than instinctive reactions and it did not construct a specific deliberative process for them to first develop and then reflect on their understanding of the area, other than what took place in the group discussion (cf Bradwell, 2010). In this design, expert focus groups are understood as a means of accessing the views of those professionals whose daily activities shape privacy and consent in practice, an area of inquiry that is still relatively under-researched.

The groups were semi-naturally occurring ones. The identifying “themes” for two of the categories of focus groups (“representatives from civil society organizations” and “data protection professionals”) were taken from key stakeholder groups who were represented on the project’s User Advisory Group, whilst others (“Public sector organizations” and “Small and medium sized enterprises”) were based mainly on convenience, that is, participants were selected on the basis of contacts known to project participants, suggestions from the project’s User Advisory Group and project mentors. The initial invitation list was supplemented by suggestions of “friends-of-friends”. This resulted in participants in a particular focus group typically sharing a common perspective on the issue and, in some cases, they knew each other well.

In designing our selection criteria, whilst it was thought that data protection professionals would be likely to provide a perspective on consent that is based on issues that they face in the organizations they work for, we felt that civil society organization representatives would be in a position to problematize consent, including highlighting the problems faced by individuals who can contact them directly. The public sector in the UK is one of the largest users of personal data, and for many government functions, consent is not actually required. In contrast, the SME focus group was selected because many SMEs have limited organizational resources to address non-core issues and we expected that privacy and consent could be one such issue that they might have limited knowledge of.

The four expert focus groups were held between November 2008 and February 2009, see Table 1.

	Date	Number of participants	Duration	Transcript size (words)
1: Civil society organizations (CSO)	November 2008	8	3 hours	25,000
2: Data protection professionals (DPP)	January 2009	11	3 hours	27,000
3: Public sector organizations (PSO)	February 2009	9	3 hours	22,000
4: Regional technology cluster: Small and Medium Sized Enterprises (SME)	February 2009	23	1 hour	16,000
Total			10 hours	90,000

Table 1 Focus group details***The EnCoRe expert focus groups: Designing the process***

As we mentioned earlier, the literature on focus groups recommends that groups are composed of at least six participants. Very large focus groups can be unproductive because it could be difficult to include contributions from all participants. Since controlling the dynamics of focus groups can require specialist skills for this study a professional, external facilitator, Tim Morley from KnowInnovation, was hired to facilitate all the focus groups.

Tim had been part of the team that ran the Sandpit event where the EnCoRe project proposal was initially developed. Despite his initial exposure to the problem area, throughout the study he told focus group participants that he was an expert on process rather than content. (In practice, however, Tim also made helpful content suggestions during informal discussions outside of the focus groups and suggested a number of useful examples and links. In similar vein, productive engagement with non-participants arose with our transcribers who also sent links to news stories that they felt would be of interest to the project).

Audio and video recordings were made of the focus groups (although the videos were used simply to aid the transcription process and were destroyed after the transcription was complete). In addition to the facilitator, participants and the first author as the note-taker, each focus group had one or two project researchers sitting in on the event. Although they were invited to participate in the discussion, they typically held back and acted simply as observers and hence had minimal impact on the content and flow of the discussions. Most of the focus groups were hosted at the first author's institution. Travel expenses were paid for participants if required.

Focus group 4 took place at the location of one of the other project partners, as part of a networking event for a regional SME technology cluster. The event was sponsored by the local business development agency. After a networking buffet, the first hour was the focus group and this was followed by a one hour presentation about privacy and consent by the first author.

As regards recruitment, the invitation to the focus group gave brief details of the project as well as practicalities of the event. The focus groups typically began with a sandwich lunch, during which time participants could meet each other and the facilitator. The formal focus group began with a brief outline of what the focus group was trying to achieve. Participants were told that there were no “right answers” but that, instead, the project was interested in learning their expert opinions about the topic. Participants asked to sign a consent form and were told that the session was being recorded. They were also told that “The discussions will be recorded, transcribed and analyzed for key themes that emerge from the discussion. The data from the session will be available to all researchers working on the project but the transcripts will be kept anonymous. The data may also be used in reports and publications and direct anonymized quotations from the transcript may be used in published output”. For the three-hour focus groups, a coffee break was scheduled for approximately two-thirds of the way through.

Although interview agendas are commonly developed to structure focus group discussions, we developed a series of “use case” scenarios for these expert focus groups instead. These scenarios used to trigger discussion about particular issues. For example, Scenario 3 was explicitly about “Terms and Conditions” on websites and Scenario 9 about “Company ownership” raised issues about use of customer data when the ownership of a company changes (cf BBC News, 2010b). These scenarios were shared with the focus group facilitator in advance of the focus groups. Tim typically began the focus groups with an open question along the lines of “in terms of consent, what keeps you awake at night?” and kept the conversation flowing drawing on the themes from the scenarios (even though, in practice, they were only explicitly used in one of the focus groups). In addition, Tim and the first author used the coffee breaks to ensure that the focus groups were not missing any important issues.

The EnCoRe expert focus groups: Developing the Analysis

Transcripts of the focus groups were produced by a trusted commercial transcription company who destroyed their copies of the audio and video recordings once the transcription was complete. The transcripts were hosted on a secure project server alongside the audio recordings. For this study, the transcription process was focused rather on what was uttered than who uttered particular statements. No attempt was made to identify patterns in the statements as made by particular individuals.

A range of analysis methods were used. Formal coding of the transcripts was done using the Atlas.ti qualitative analysis software (version 6.1.12). The transcripts were loaded into Atlas.ti and all the relevant text was coded, in a bottom up (but not necessarily grounded theory) approach each (cf Urquhart et al., 2010). The nature of our expert focus groups meant that pre-existing codes did not exist—and they would not necessarily have been helpful given the diverse expertise between the groups. As the focus groups were relevant to a variety of project activities, all the text of the transcripts was coded. The codes were normally allocated to a “paragraph” of the transcript, although occasionally the code would run over a number of related paragraphs. Some paragraphs, naturally, had a number of different codes allocated to them (Olivero & Lunt, 2004). This initial coding process resulted in over 850 distinct codes.

A key step towards consolidating codes into analytically distinct segments that can be examined together both within and between groups (Knodel, 1993) involved tidying up the initial codes, for example by combining codes that covered the same concept but were labeled slightly differently. For example, the code “Personal benefit of data sharing” was felt to convey the same ideas as the code “We don’t like data being used but like the business benefits” and so the two sets of codes were merged. The analysis was also based on, and contrasted with, themes from the literature (Knodel, 1993; Eisenhardt, 1989) and involved an iterative process of reading, coding and cycling through the

codes (Frankland & Bloor, 1999). The validity of the coding and analysis was constantly checked by searching for counter examples and nuances in the transcripts and codes.

The next stage in the analysis was to create what Atlas.ti calls Code Families. Initially these code families were fairly generic, for example, one code family consisted of all the codes related in any way to the notion of consent, another to all mention of the use of “terms and conditions”.

These high level code families were then broken into constituent elements. For example, the code family “Consent” consisted of over 90 individual codes. The Network View tool allowed these individual codes to be categorized further, for example the codes associated with the overhead of gaining clear informed consent. This process also led to further consolidation of codes.

In the remainder of the paper, a selection of coded quotations is presented. Each quotation is accompanied by a two-part code. The first part indicates the focus group it was taken from using the codes presented in Table 1 (CSO, DPP, PSO, SME). As the transcripts and analysis explicitly did not include details of which participant made the utterance, the second part of the code, refers to the paragraph number that the quotation was taken from rather than the speaker. As the raw data is transcription of the natural conversation, some work has been undertaken to make the quotations more legible. Clarifications and additional words are presented in square brackets, transcription annotations are in curly brackets.

For example, the following quotation was made in the Civil Society Organizations focus group; it refers to a Facebook group. The quotation is in paragraph 615 of the transcript.

I’m only in one [Facebook] group, I’m in a group called “Che Guevara was a murderer and your t-shirt isn’t cool”. {LAUGHTER} That’s the only group I’m in. [CSO 615]

Green and Hart (1999) argue that the “face validity” of focus groups (Marshall & Rossman, 2006) can be enhanced by properly contextualizing the extracts, showing not only “what was said” but also how the conversation led to it being said. This also helps highlight the particular ways in which focus groups can bring out emergent views on a topic. In this paper, italics are used to differentiate between statements made by different participants (where it is possible to discern that more than one participant contributed to a particular discussion thread).

This extract follows from a discussion about one of the participant’s son using Facebook:

How old is he?

He’s 14 and he’s on Facebook every night, right, because that’s, that’s what kids do. So first of all he wouldn’t let me be his friend cos it’s like it’s not nice when people’s parents are their friends ...

Once the coding process was complete, the resulting codes, code families and quotations were made available to all project members via an interactive website. This allowed individual researchers to explore the different codes and code families and “explode” them to view the underlying quotations from the interviews. This enabled further informal analysis by two other members of the research team who read through all of the transcripts and used their engagement with the material to confirm, clarify or challenge the main interpretations presented here. Those members who sat in on the various focus groups were also able to raise pertinent themes from the focus groups in project meetings (“This reminds me of something that was mentioned at the focus group I attended ...”).

Results

All four focus groups generated important insights for our research questions currently grouped into three themes for the purposes of this paper. The discussion of these themes below is complemented by an examination of our initial research question to test the concept of informed consent in online interactions. Example quotations are given for each of the themes. There was a tendency for the CSO focus group participants to focus more on privacy policies and effective control over personal data, whilst the commercial participants in the other focus groups concentrated their attention on consent as a regulatory requirement and on the controls that they have over the use and misuse of personal data.

Theme 1. Privacy policies, terms and conditions

The first theme relating to the detailed research questions addresses the extent to which consent might be truly “informed” in online interactions. Although some empirical studies suggest that the existence of a privacy statement could be sufficient to address the privacy concerns of data subjects, the evidence from the focus groups calls into question the extent to which privacy policies provide adequate information to potential data subjects. The focus groups problematize and question the extent to which anyone even looks at privacy policies and, if they do, whether they are able to read the material found there and whether it adequately details the aims and methods of the service provider and the benefits and risks of the interaction. Whereas one might think that this an obvious point to raise, it is in fact an important one to provide concrete evidence on, both as regards the public and private sectors.

A core consideration with privacy policies that was important for focus group participants is *the way in which they are presented* to the data subjects. For example, one participant noted:

I just showed you on Facebook the terms and conditions on my Blackberry, which nobody ever will read, the only thing in big letters is the “I Accept” button, you know, so, so before you can do any, you know, any, any meaningful consent you’ve got to address the issue of how aware people are, consumers are, users are, about what’s collected about them, how it is used, for what purposes and how ... what can they do about it, because most people have no clue. [CSO 847]

Suggesting that:

the information about privacy given to them is completely useless and they don’t use it. [CSO 847]

and that:

you needed a reading age of like 27 to read the average privacy [policy]. [COS 849]

A participant in the Public Sector Organization focus group spoke about the consent they collect from citizens:

We collect consent from the informant that first of all they are either the next of kin or they are authorised to act on [their] behalf. We collect consent at the end that they understand that the data is going to be used to amend or adjust entitlements to benefits and services and this catch-all phrase, which is actually “And the receiving departments may use it in ways which they are legally able to do so,” which isn’t ideal, but it sort of gets the message across without having a four-page disclaimer about surveys certain bits of government might be doing at any given time. [PSO 420]

As an illustration of this theme, the computer game seller Gamestation briefly updated their terms and conditions of sale on 1 April 2010. In the revised terms and conditions they claimed the legal rights to the souls of any customers who bought from them that day. The new conditions said that “By

placing an order via this web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, your immortal soul”. Although 7500 customers bought games that day, none clicked on the link that allowed them to nullify the sub clause and proceed with the transaction (OUT-LAW, 2010).

Theme 2. Effective control over the use of personal data

If one makes the bold assumption that data subjects have read and understood the privacy policy or terms and conditions that the service provider initiates, to what extent do they have control over how their data is handled in practice? Again the evidence from the focus groups suggests that even in these circumstances, the effective control that data subjects can exercise is limited in a variety of ways.

For example, one participant noted that the current set up favors involuntary consent:

I mean for example just to follow from what [...] was saying, if you for a start have a user-friendly format design that actually makes people aware that they are giving consent or not, which is not happening at the moment, at the moment you've got pre-ticked boxes and every possible way to avoid informed consent, you know, you have involuntary consent. Well, if that got put right in the first place you would have a huge progress. [CSO 279]

Another practical problem that arises in the public sector is that the nature of *relationship* between the citizen and the State means that:

what I was talking about switching on and off is [Government Department] sharing a piece of information with [Another Government Department] or with the local authority or whatever. It's the permission to share or even the request, "Please will you go and share" they'd be switching on and off rather than any particular obligation to notify somebody about a change of circumstances, which is still a legal responsibility.

Yeah, I take that, but we still work in a world where those, actually the citizen currently, in some areas, has no right to give permission anyway, because there is a legal power for some of those bits of data to be shared whether the citizen gives consent or not. [PSO 87–89]

Although Data Protection is regulated in the UK by the Information Commissioner, it was generally felt that his powers were *rather limited*. So if the only constraint on an organisation that was about to misuse personal data was penalties from the ICO, then:

effectively they can operate with impunity, they can do whatever the hell they please when it comes to the crunch, you know, in real world consent, revocation, they can do whatever they want and the individuals are in no position to do anything about it. The consent that they've given actually becomes meaningless ... [DPP 111]

Another limitation on effective control was the recognition that if the particular data processing was stated and legitimate, then the data subject had *little recourse*:

Providing [the undesired data process activity is] done for legitimate business purposes and provided the 3rd party that they're providing the information to is reminded of their responsibilities under the Data Protection Act then as a business you should be covered. [DPP 595]

Unintended collection or processing of personal data was also raised. Interestingly, in this case, the data processor used the realization that they had access to such data to improve their reputation with the data controller:

After that little incident where I discovered I'd got a large number of usernames and passwords in the clear, I said well, I can use this to my advantage to give the client some visibility of that I'm quite ethical about these things and as a policy we erase all data when it's completed, we provide the client with a certificate of destruction and we use some PGP software to make sure that we have erased all the data, because I just don't want it, that's a liability. [SME 227]

Other SMEs recognized the *value of the data* that they collect which runs counter to the desire for control on the part of the data subjects:

As data collectors we want that information. We want to keep it as long as we can, because that's part of the IT sort of ethos. If I can gather data on this customer, he uses this kiosk at this time, that kiosk at that time, or that terminal at that time, or buys online at time, that data's important to me, or hugely more important to my clients. So I'll try and get away with as much as I possibly can, without making it too unsecure. [SME 85]

Theme 3. Consent as a response to regulatory requirements

An important concern about the use of informed consent in online transactions arises when it is sought in order to ensure compliance with the relevant regulatory requirements rather than to address basic questions of personal autonomy and human dignity. In the UK, this means compliance with the requirements of the UK Data Protection Act. In other jurisdictions this may be compliance with the GAPP or Fair Information Practices. Again, the experts in our focus groups highlighted the extent to which this was the case.

Organizational adherence to privacy policies was an issue raised at the SME focus group:

I think one slight pitfall that some employers go into, I speak from a past life, is that they [have] to have the [Data protection] policies, but the onus is on them to communicate and to let their employees know that they understand or at least sign something to say [that they do] ... You might have a policy but you don't actually follow it and that happens a lot in organisations that I've been working with. ... Generally we say to people you're better off to have no policy than have a policy and not follow it. [SME 253, 261, 263]

Another concern was whether organizations would *adopt best practice* "or just go for minimal compliance or in fact not even bother doing that, as does happen?" [DPP 77]. Even minimal compliance was considered an attractive option because "the UK [Data Protection] Act is the most friendly act in ... of all the, you know, the EU". "[It] lets you get away with anything you want", "Exactly. Exactly right, you can do anything you want". [DPP 121–123]

Regulatory compliance was also an issue for small and medium sized enterprises:

I think the reality as most small businesses when you start out there's a great deal of ... a very large amount of, I'll call it administrative overhead in an organisation, that we know exists in the enterprise and that we know that as small businesses we should be doing it but many of us simply don't, because you've not got the time, you've not got the knowledge, you require that extra expertise. But there comes a point where you have to start taking these things on board and I'm not sure where in the SME life ... you know, where our growth that actually is. I'm certainly not worried, not worried about it yet. [SME 66]

When these organizations were required to implement data protection systems, they did so to the *standard* required of their commercial partners, not necessarily that of the law, for example in the case of handling payments:

I mean the information is not 100% clear because we're dealing with 3rd party payment gateway and some payment gateways have some rules, about how long we can store data, and other, other companies have different rules. Now we have to comply with their rules, not necessarily with the

government standards. Now they could be more than the government standards or depending on the company, slightly less. [SME 72]

Data protection was described as “quite poorly understood in British boardrooms ...” [DPP 213] and decisions were frequently taken that:

could be deemed as fairly undesirable by the data subject, cos they’re answerable to shareholders not to the public. [DPP 217]

Even softer forms of regulation, such as *voluntary codes of conduct* were being challenged by the effects of the recession:

Yeah, I think we’re also seeing it the commercial arena these things are failing. You know, the DMA [Direct Marketing Association] opt-outs and all the Codes of Practice around that we’ve been ... you guys must have the same, there’s probably a credit crunch symptom is companies now are just disregarding DMA Codes of Practice, they’re phoning anyone at any hour of the day. [DPP 165]

Another perceived problem was that the current Data Protection legislation was “incredibly poorly drafted” and would take somebody doing it full time “7 years to get their head around how the legislation is supposed to work” [DPP 739]. Another participant noted:

I very well remember the initial agonies and feeling I was a complete dunce most of the time, and one of the reasons why I said ... it is in some ways poorly drafted, but it’s also problems because of the scope of it, because it applies to everything, initially, absolutely everything and then it progressively rows back from that initial declaration, you know, a universal application through the exemptions, through the special rules, the special kinds of data and so on and the difficulty really is getting from that first point, you know it applies, to working out how it does apply in this particular instance that you’re faced with. That’s the difficult journey. That’s the journey that most of the guidance tries to help people with doesn’t help with. [DPP 741]

Testing the nature of informed consent

The evidence gathered from our expert focus groups strongly indicates that *informed consent rarely functions well* in online interactions in the sense that it is unlikely to be truly informed and freely given. This was perhaps most articulately presented by a participant in the Data Protection Professional’s focus group, who said:

I mean I know when I did my ISEB [Information Systems Examinations Board] training one of the things I was told was that processing under consent is what the desperate resort to {LAUGHTER}. In other words it’s the last thing you ever want to process personal data under. [DPP 909]

In other cases consent was seen as something that was *sought, even if it wasn’t required*:

Yeah, I mean one of things I think about consent, and it seems to me in a lot of cases, people ask for consent when in fact it’s not really consent because one of the things about consent is it has to be free given. So if you, for instance, went into an NHS [National Health Service] hospital—not that I’ve been in one recently anyway—but and they say to you, “Oh you need to sign this form, because, you know, we may need to pass your data round, blah, blah, blah, blah,” you say “Well, no I’m not signing that form,” and they say “Well, we can’t treat you then,” I think there’s an argument that’s not really consent is it, you know, because you’re gonna, you know, “I’ll stand here and drop dead then” ... {SEVERAL SPEAK} It’s not likely, so I think there are some confusion, you know, I think consent really should only ever be asked for, you know, when it clearly is freely given as a choice of the individual otherwise it’s not consent and we’re just kidding ourselves. [DPP 161]

Similarly, when people such as employees, complain that the organization needs their consent before doing anything with their data then:

99% of the time you don't because you're processing it under legitimate interests and I have found quite a lot of confusion amongst employees who are sending me emails and ringing me up saying, you know, well, you know, you never asked my consent to do this processing, blah, blah, blah, blah, blah and I have to explain to them, it's quite a difficult conversation, cos they don't like the answer that we don't need their consent, that, you know, as long as we have a legitimate business need and we have, you know, been transparent with them, which we always are in terms of who we're sharing the data with, why it is, what the business reason is, we don't need their consent. [DPP 593]

A further nuance about the nature of informed consent was also raised in this focus group as regards understanding the risks of *data relocation*:

It's almost impossible for most data subjects to actually give informed, valid consent to this [a situation where a company was planning to relocate its data centre out of Europe], they don't understand the risks, you know, unless you presented me with a full risk analysis of what's been done for this data centre in Moscow and how it's going to be handled and what the regulations are, and I can understand that, how can I give valid consent to that data transfer? [DPP 77]

Discussion

This paper presents research undertaken as part of a project investigating aspects of consent in online interactions. The fieldwork that is reported here is based on a series of focus groups that were undertaken with various experts in privacy policy and data protection practice.

Previous sections of this paper have highlighted the utility of this particular form of focus group, namely the expert focus group, for privacy research and information systems research more generally. This section discusses the implications of the research conducted with these focus groups to date and revisits the tentative definition of informed consent hypothesized at the start of the paper. The evidence from the expert focus groups suggests that this definition would be of limited applicability to the practice of many online interactions in terms of the behaviors of both data subjects and data controllers. The paper proposes an alternative way of conceptualizing consent on the basis of these considerations. In our introductory discussion of informed consent at the beginning of the paper, a *definition* of informed consent for online interactions was contemplated, based on the World Medical Association's definition:

In online interactions, each potential data subject must be adequately informed of the aims and methods of the service provider, the anticipated benefits and potential risks of the interaction and any other relevant aspects of the interaction. The potential data subject must be informed of the right to refuse to participate in the interaction or to withdraw consent to participate at any time without reprisal. Special attention should be given to the specific information needs of individual potential data subject as well as to the methods used to deliver the information. After ensuring that the potential data subject has understood the information, the organization must then seek the potential subject's freely-given informed consent.

The evidence from the expert focus groups indicates a number of areas where such a definition would inadequately represent current practice regarding informed consent for online interactions in the UK. The key areas of inadequacy are discussed below, together with implications for further research and practice in the area of informed consent.

In terms of an obligation for a data processor and / or controller to *keep the data subject "adequately informed"*, our focus group evidence highlights the following problems with current manifestations of

informed consent. Most current privacy policies are effectively unreadable and hence unread. Thus whilst they might satisfy the letter of regulatory constraints found in the UK (or the openness principle of the OECD guidelines more generally) their mere existence fails to address the spirit of informed consent described above. The recent guidance on privacy notices by the UK Information Commissioner as well as recent work that seeks to present privacy risks in novel ways (e.g. Kelley et al., 2010) open up important avenues for future research as regards the extent to which such new approaches can help keep data subjects adequately informed of the aims, methods, benefits and risk of online interactions, by considering their with various information needs and processing capabilities). This approach implies a reevaluation of many of the privacy instruments used for empirical research. If hardly anyone reads privacy statements / terms and conditions for online services and those who do find them of limited utility in informing their decisions, then the extent to which procedural fairness might increase trust in online transactions needs to be reconsidered.

Although consent plays an important role in academic and policy based discussions of privacy (e.g. Culnan & Armstrong, 1999; BCS, 2009; Petty, 2000) less emphasis is given on the *right to refuse* to participate in an online interaction or the *right to withdraw* consent to participate at any time without reprisal (Curren & Kaye, 2010). This is particularly the case for a significant number of interactions where consent is not required (e.g. interactions with the public sector) or where organizations have explicitly sought to structure their interactions with customers so as to obviate the need to obtain the consent of the data subject. There is a need for further research to map out the extent of *consent-less processing* of personal data and to assess the extent to which this is driven by corporate management, national regulation, or other concerns (cf Milberg et al., 2000).

A further problem with freely given informed consent is the extent to which institutional or market forces offer the data subject a *meaningful choice of options*. For example, consent given in a situation with few realistic alternatives cannot be considered to be freely given. An illustration of this problem can be seen in the Manuscript Central privacy policy. This was updated on 6 July 2010 (the previous version was dated June 2006). It states that the Privacy Policy may be revised periodically and advises that data subjects review the policy “*whenever you visit the Website* so that you are aware of any changes. Your continued use of the Website following any changes in this Privacy Policy will constitute your acceptance of such modifications” (emphasis added). It continues by noting that:

Your use of the website constitutes your unconditional acceptance of the practices described in this privacy policy and the other terms and conditions of the terms of use. If you do not agree with and accept all of the practices described in this privacy policy, do not use the website or do not provide or submit any personally identifiable information via or while using the website, the software, or the services (Manuscript Central, 2010 Capitalization removed for presentation purposes).

Manuscript Central is used by many of the leading information systems journals (MISQ, ISR, ISJ, JAIS) and conferences (ICIS 2010, ECIS 2010, AMCIS 2010). Thus academics who wish to publish their work in these leading outlets *must* accept the practices in the Manuscript Central privacy policy. Whilst there is no reason to suggest that there are any issues with Manuscript Central’s privacy policy, use of the system hardly fits within the notion of “freely-given” informed consent. If these journals and conferences are going to continue to use Manuscript Central, then they should offer an alternative submission (and review) system for those academics who are not prepared to “agree with and accept all of the practices” in the privacy policy.

In terms of practice, being able to provide evidence that users “ticked the box” or “opted-in” to a particular service hardly addresses the underlying argument for informed consent in terms of basic

human dignity if the consent has limited validity. A decrease in data quality could be one potential consequence. If data subjects, who wish to use an online service, believe that the service provider is collecting unnecessarily detailed information or if there is a perception that the data will be misused, then a likely response will be for those data subjects to lie in their data entry: if requested for their date of birth when it is not apparent why it is needed, they might enter 1 April for their birthday, or enter the correct day and month but an incorrect year. The consequences of such poor data quality for business intelligence, tailored marketing etc. could be significant (Bertini, 2010).

In conclusion: Rethinking consent?

If consent and procedural fairness, as conventionally understood, are proving to be inadequate for online interactions the most effective solution might be to *rethink consent*. For example, rather than focusing on trying to perfect the initial consent (which itself could be “engineered” for particular organizational goals (Kerr et al., 2009)) it might be more appropriate to accept that initially given consent might not be optimal and might need to change over time and thus emphasize consent management as an ongoing activity rather than as a one-off event. This rethink would require a model of consent to be not static, as current models are, but instead a fluid, *ongoing, dynamic process* that can be followed and reliably changed over time.

The data subject might *change their mind* about consent that has been given and wish to revoke or refine that consent at a later stage. Although much lip service has been given to providing data subjects with more control over their personal data (Curren, 2010; Whitley, 2009), in practice this tends to be restricted to controlling the initial disclosure of the data or allowing a partial opt-out at a later stage. Such opt-outs are typically limited to no longer sending the data subject marketing messages whereas, in practice, revocation of consent should mean that the data subject’s personal data should be put out of use so that it is unusable for the organization.

More *sophisticated mechanisms of revocation*, however, might include deletion of the data held on the company servers (and back-up tapes) or one-way escrowed encryption of the data. In each case, an auditable proof of revocation will be needed, both for the data subject and other third party data controllers. The EnCoRe project is currently investigating ways in which dynamic and granular options for revocation can be developed and implemented in system design as well as in governance mechanisms. It is currently planning a pilot qualitative study to gather lay-user views and expectations on revocation in the context of biobanking.

A further issue in need of additional research is the distinction between requirements of procedural fairness vis-à-vis expectations of user control in online interactions. Both terms can be expressed as positive and negative claims. For example, procedural fairness can be described in (negative) terms of not using data in ways that will harm the data subject, or in (positive) terms of notifying the data subject about the use of their data according to fair processing principles. Similarly, control can be conceptualized in (negative) terms of not sharing data with third parties other than the designated parties by the user, in line with their consent preferences, or in (positive) terms of using the data in ways that recognize the data subject’s contribution, that is, as ways in which the data subject makes a difference. As part of the pilot study to investigate user attitudes about revocation, the EnCoRe project will also undertake further research to test user views on the desirability of control in positive terms.

References

- AICPA (2010) Generally Accepted Privacy Principles AICPA Archived at <http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy+Principles>
- Albrecht TL, Johnson GM and Walther JB (1993) Understanding communication processes in focus groups. In *Successful focus groups: Advancing the state of the art* (Morgan DL, Ed), pp 51-64, Sage, London.
- Allen AL (1999) Coercing privacy. *William and Mary Law Review* 40(3), 723-757.
- Angst CM and Agarwal R (2009) Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion. *MIS Quarterly* 33(2), 339-370.
- Awad NF and Krishnan MS (2006) The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly* 30(1), 13-28.
- BBC News (2010a) Google admits Buzz social network testing flaws (16 February) Archived at <http://news.bbc.co.uk/1/hi/technology/8517613.stm>
- BBC News (2010b) Privacy fears over gay teenage database (13 July) Archived at <http://www.bbc.co.uk/news/10612800>
- BCS (2009) Personal data guardianship code *British Computer Society* Archived at <http://www.bcs.org/upload/pdf/pdgc.pdf>
- Bertini P (2010) Trust me! Explaining the relationship between privacy and data quality. In *ItAIS 2010*, Italy.
- Bonner W and Chiasson M (2005) If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization* 15(4), 267-293.
- Bradwell P (2010) *Private lives: A people's inquiry into personal information*. DEMOS, London.
- Bygrave LA (2002) *Data protection law : approaching its rationale, logic and limits*. Kluwer Law International, The Hague ; London.
- Collins V (1993) Privacy in the United Kingdom: A right conferred by Europe. *International journal of law and information technology* 1(3), 290-304.
- Culnan MJ (1993) "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly* 17(3), 341-363.
- Culnan MJ and Armstrong PK (1999) Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation *Organization Science* 10(1), 104-115.
- Culnan MJ and Williams CC (2009) How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly* 33(4), 673-687.
- Curren L (2009) Data protection law and the legal basis of privacy *EnCoRe Project Briefing Paper*
- Curren L (2010) User-centric models of personal data processing: A discussion of the related law, policy and technology *EnCoRe Project Briefing Paper*
- Curren L and Kaye J (2010) Revoking consent: A 'blind spot' in data protection law? *Computer Law & Security Review* 26(3), 273-283.
- De Hert P (2008) Identity management of e-ID, privacy and security in Europe. A human rights view. *Information Security Technical Report* 13(2), 71-75.

EnCoRe: Ensuring Consent and Revocation

- DeCew J (1997) *In pursuit of privacy: Law, ethics and the rise of technology*. Cornell University Press, Cornell.
- Eisenhardt KM (1989) Building theories from case study research. *Academy of Management Review* 14(4), 532-550.
- EU (2008) Opinion 1/2008 on data protection issues related to search engines *Article 29 Data Protection Working Party* Archived at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf
- Fern EF (1982) The use of focus groups for idea generation: The effects of group size, acquaintanceship, and moderator on response quantity and quality. *Journal of Marketing Research* 19(1), 1-13.
- FIPR (2009) Database state: A report commissioned by the Joseph Rowntree Reform Trust Ltd (22 March) Archived at <http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf>
- Fiveash K (2010) Google Buzz leaves privacy concerns ringing in ears (11 February 2010) Archived at http://www.theregister.co.uk/2010/02/11/google_buzz_privacy/
- Frankland J and Bloor M (1999) Some issues arising in the systematic analysis of focus group materials. In *Developing focus group research: Politics, theory and practice* (Barbour RS and Kitziinger J, Eds), pp 144-155, Sage, London.
- Gibbs A (1997) Social research update: Focus groups *Sociology at Surrey* Archived at <http://sru.soc.surrey.ac.uk/SRU19.html>
- Green J and Hart L (1999) The impact of context on data. In *Developing focus group research: Politics, theory and practice* (Barbour RS and Kitziinger J, Eds), pp 21-35, Sage, London.
- Hoeyer K (2009) Informed consent: The making of a ubiquitous rule in medical practice. *Organization* 16(2), 267-288.
- Hoffman D, Novak T and Peralta MA (1999) Information privacy in the market-space: Implications for the commercial use of anonymity on the web. *The Information Society* 15(2), 129-139.
- Hoofnagle CJ, King J, Li S and Turow J (2010) How different are young adults from older adults when it comes to information privacy attitudes & policies *UC Berkeley* Archived at <http://www.ftc.gov/os/comments/privacyroundtable/544506-00125.pdf>
- Hui K-L, Teo HH and Lee S-YT (2007) The value of privacy assurance: An exploratory field experiment. *MIS Quarterly* 31(1), 19-33.
- Information Commissioner's Office (2009) Privacy notices code of practice *ICO* Archived at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_notices_cop_final.pdf
- Information Commissioner's Office (2010) About us *ICO* Archived at http://www.ico.gov.uk/about_us.aspx
- Introna LD (1997) Privacy and the computer: Why we need privacy in the information society. *Metaphilosophy* 28(3), 259-275.
- Jackson E (2009) *Medical law – Texts, cases, and materials*. Oxford University Press, Oxford.
- Junglas IA, Johnson NA and Spitzmuller C (2008) Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems* 17(4), 387-402.
- Kanellopoulou N (2009) Legal philosophical dimensions of privacy *EnCoRe Project Briefing Paper*
- Katz J (1992) The consent principles of the Nuremberg Code: Its significance for then and now. In *The Nazi Doctors and the Nuremberg Code* (Annas GJ and Grodin MA, Eds), pp 227–239, Oxford University Press, Oxford.

- Kelley PG, Cesca L, Bresee J and Cranor LF (2010) Standardizing privacy notices: An online study of the nutrition label approach *CyLab, Carnegie Mellon University* (12 January) Archived at http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf
- Kerr I, Barrigar J, Burkell J and Black K (2009) Soft surveillance, hard consent: The law and psychology of engineering consent. In *Lessons from the identity trail: Anonymity, privacy and identity in a networked society* (Kerr I, Steeves V and Lucock C, Eds), pp 5-22, Oxford University Press, Oxford.
- Kitzinger J (1994) The methodology of focus groups: The importance of interactions between research participants. *Sociology of Health and Illness* 16(1), 103-116.
- Kitzinger J (1995) Introducing focus groups. *British Medical Journal* 311(7000), 299-302.
- Knodel J (1993) The design and analysis of focus group studies: A practical approach. In *Successful focus groups: Advancing the state of the art* (Morgan DL, Ed), pp 35-50, Sage, London.
- Krueger RA (1988) *Focus groups: A practical guide for applied research*. Sage, London.
- Krueger RA (1993) Quality control in focus group research. In *Successful focus groups: Advancing the state of the art* (Morgan DL, Ed), pp 65-88, Sage, London.
- Kuner C (2003) *European data privacy law and online business*. Oxford University Press, Oxford.
- Law J and Mol A (Eds.) (2002) *Complexities: Social studies of knowledge practices*. Duke University Press, Durham.
- Light B, McGrathy K and Griffiths M (2008) More than just friends? Facebook, disclosive ethics and the morality of technology. In *International Conference on Information Systems (ICIS)*, Paris.
- Lundblad N and Masiello B (2010) Opt-in Dystopias. *script-ed* 7(1),
- Malhotra NK, Kim SS and Agarwal J (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research* 15(4), 336-355.
- Manuscript Central (2010) ScholarOne Manuscripts Website Privacy Policy Statement (6 July) Archived at <http://mc.manuscriptcentral.com/downloads/privacy.htm>
- Marshall C and Rossman GB (2006) *Designing qualitative research*. Sage, London.
- Mason K and Laurie G (2006) *Law and medical ethics*. Oxford University Press, Oxford.
- Milberg SJ, Smith HJ and Burke SJ (2000) Information privacy: Corporate management and national regulation. *Organization Science* 11(1), 35-57.
- Morgan DL (Ed.) (1993) *Successful focus groups: Advancing the state of the art*. Sage, London.
- Moskop JC (2007) Information Disclosure and Consent: Patient Preferences and Provider Responsibilities. *The American Journal of Bioethics* 7(12), 47-49.
- OECD (1980) Guidelines: On the Protection of Privacy and Transborder of Personal Data *Organisation for Economic Co-Operation and Development* Archived at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
- Olivero N and Lunt P (2004) Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of economic psychology* 25(2), 243-262.
- Open letter (2010) Open letter to Eric Schmidt, Chairman and CEO of Google Archived at http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf

EnCoRe: Ensuring Consent and Revocation

OPSI (1998) Data Protection Act.

OUT-LAW (2010) Nobody reads terms and conditions: It's official Archived at <http://www.out-law.com//default.aspx?page=10929>

Pavlou PA (2003) Consumer acceptance of electronic commerce: Integrating trust and risk with the Technology Acceptance Model. *International Journal of Electronic Commerce* 7(3), 101-134.

Pavlou PA, Liang H and Xue Y (2007) Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly* 31(1), 105-136.

Perecman E and Curran SR (2006) *A handbook for social science field research : Essays & bibliographic sources on research design and methods*. Sage, London.

Petty RD (2000) Marketing without consent: Consumer choice and costs, privacy and public policy. *Journal of Public Policy and Marketing* 19(1), 42-53.

Pollach I (2005) A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics* 62(3), 221-235.

Smith HJ, Milberg SJ and Burke SJ (1996) Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20(2), 167-196.

Son J-Y and Kim SS (2008) Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly* 32(3), 503-529.

Tams S and Grover V (2010) The effect of an IS article's structure on its impact. *Communications of the AIS* 27(10),

Thaler RH and Sunstein CR (2008) *Nudge: Improving decisions about health, wealth and happiness*. Penguin, London.

Tremblay MC, Hevner AR and Berndt DJ (2010) Focus groups for artifact refinement and evaluation in design research. *Communications of the AIS* 26(27), 599-618.

Tsai JY, Egelman S, Cranor L and Acquisti A (2010) The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* Forthcoming,

U.S. Department of Health Education and Welfare (HEW) (1973) Records, computers and the rights of citizens: report of the Secretary's Advisors Committee on Automated Personal Data Systems *U.S. Government Printing Office* Archived at <http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm>

Urquhart C, Lehmann H and Myers MD (2010) Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in information systems. *Information systems journal* 20(4), 357-381.

Veatch RM (2007) Implied, presumed and waived consent: The relative moral wrongs of under- and over-informing. *The American Journal of Bioethics* 7(12), 39-41.

Warren S and Brandeis L (1890) The right to privacy. *Harvard Law Review* 4, 193-220.

Whitley EA (2009) Informational privacy, consent and the "control" of personal data. *Information security technical report* 14(3), 154-159.

Wilkinson TM (2001) Research, informed consent and the limits of disclosure. *Bioethics* 15(4), 341-363.

Williams M (2003) *Making sense of social research*. Sage, London.

World Medical Association (1964) Ethical Principles for Medical Research Involving Human Subjects *World Medical Association* Archived at <http://www.wma.net/en/30publications/10policies/b3/17c.pdf>

EnCoRe: Ensuring Consent and Revocation

Younger Committee (1972) Report of the Committee on Privacy *HMSO*

Zeps N, Iacopetta BJ, Schofield L, George JM and Goldblatt J (2007) Waiver of individual patient consent in research: when do potential benefits to the community outweigh private rights? *MJA* 186(2), 88-90.

ⁱ In this paper, the term “Data Subject” (taken from the UK Data Protection Act 1998) refers to the citizen / consumer / user of an online service. The “Data Controller” is the organization who is (legally) responsible for the processing of the data (the actual implementation of which might be delegated to a separate “Data Processor”).